

The diameter of a random Cayley graph of Z_q

Gideon Amir ^{*} Ori Gurel-Gurevich [†]

October 4, 2009

Abstract

Consider the Cayley graph of the cyclic group of prime order q with k uniformly chosen generators. For fixed k , we prove that the diameter of said graph is asymptotically (in q) of order $\sqrt[k]{q}$.

The same also holds when the generating set is taken to be a symmetric set of size $2k$.

1 Introduction

Let G be a finite group. Let S be a subset of G . The (directed) *Cayley graph* of G (w.r.t. S) is a graph (V, E) with $V = G$ and $(g, h) \in E$ if and only if $h^{-1}g \in S$. The elements of S are then called *generators* and S the *generating set*. If S is symmetric (w.r.t. inversion) then the resulting Cayley graph is essentially undirected - if (g, h) is in E then so is (h, g) .

A "random random walk" on a group G is a random walk on the Cayley graph of G , with a generating set chosen randomly in some fashion. The random walk itself may be simple, each edge having equal probability at each step, or not simple, with some nonuniform distribution on the edges.

^{*}Department of Mathematics, University of Toronto, Toronto ON, M5S 2E4, Canada. gidi.amir@gmail.com

[†]Microsoft Research, One Microsoft Way, Redmond, WA 98052-6399, USA. orig-urel@microsoft.com

Usually, the generating set is chosen uniformly from all sets of some prefixed size k .

Various aspects, most notably the typical mixing time, of random random walks on different finite groups have been studied. (See [1, 5] for some examples, and [2] which gives a comprehensive survey). The results usually refer to Abelian groups in varying degrees of generality, from cyclic groups up to general finite Abelian groups.

Roichman ([6]) notes that the diameter of the random Cayley graph is bounded by a constant times the mixing time, and applies this bound to the case of general groups of order n and $k = \lfloor \log^a n \rfloor$. The resulting bound is $\frac{a}{a-1} \log_k n$, which is proved to be tight for the case of Abelian groups.

For the cyclic group \mathbb{Z}_n , Hildebrand [3] proved that the mixing time is of order $n^{2/(k-1)}$, and therefore, this is also a bound on the diameter of this random Cayley graph. However, in contrast with the results in [6], in this case the diameter is actually much smaller - we prove it to be $O(n^{1/k})$.

Note that as far as mixing times are concerned, there is no difference between a particular set of generators, S and the set $S + c$, attained by adding a constant $c \in \mathbb{Z}_q$ to all the generators in S . The diameter, however, might change significantly. To see this, consider, for example, a generating set of two elements, $S = \{1, \lceil \sqrt{q} \rceil\}$ in \mathbb{Z}_q (where q is prime). The diameter of this Cayley graph is $2\sqrt{q}$. Now, observe $S' = S - 1 = \{0, \lfloor \sqrt{q} \rfloor\}$. The diameter of this Cayley graph is now q . Put another way, the diameter does not change when adding or removing 0 from the generating set but the mixing time might change considerably.

Another point of notice is the question of symmetric vs. asymmetric generating sets. The results in [3] are for asymmetric generating sets, i.e. S contains just the k randomly chosen generators. We might as well ask about the mixing times and diameters w.r.t. $\bar{S} = S \cup (-S)$. The resulting random walk is now symmetric, which is sometimes more natural to consider. It seems that the results in [3], when applied to the symmetric case, would yield a mixing time of order $n^{2/k}$. In contrast, the results in this paper apply

equally to the symmetric case.

It should be noted that the asymptotic behavior of both the mixing time and the diameter, both in the symmetric and asymmetric case are the same as in the case of a k dimensional tori of volume q . This is not coincidental, the structure of the Cayley graph of G w.r.t. S is actually that of \mathbb{Z}^k , modulo some k -dimensional lattice, which contains the lattice of all multiples of q . Perhaps the mixing time results of [3] could be proved in a more elementary manner using that perspective.

2 Main results and open questions

Let \mathbb{Z}_q be the cyclic group of order q , a prime number. Let g_1, \dots, g_k be k random generators chosen uniformly and independently from \mathbb{Z}_q . Denote by $Diam(q, k)$ the random variable which is the diameter of the resulting (directed) Cayley graph. The same proofs work, *mutatis mutandis*, for the diameter of the *undirected* Cayley graph, that is, if our generating set is taken to be $\{g_1, -g_1, \dots, g_k, -g_k\}$.

A simple counting argument shows that the diameter is at least $\Omega(\sqrt[k]{q})$. We prove that the diameter is $\Theta(\sqrt[k]{q})$ in the following sense:

Theorem 1 *For all $k > 0$,*

$$\lim_{C \rightarrow \infty} \limsup_{q \rightarrow \infty} \mathbb{P}(Diam(q, k) > C \sqrt[k]{q}) = 0$$

Also, this result is tight in the sense that:

Theorem 2 *For all $k > 0$ and all C ,*

$$\liminf_{q \rightarrow \infty} \mathbb{P}(Diam(q, k) > C \sqrt[k]{q}) > 0$$

In other words, the limit behavior of the distribution of $\frac{Diam(q, k)}{\sqrt[k]{q}}$ is non-degenerate. This seems to hint at the following conjecture:

Conjecture 3 *$\frac{Diam(q, k)}{\sqrt[k]{q}}$ converges (in distribution) to some distribution $D(k)$ on \mathbb{R} which has a non-compact support.*

If this conjecture is true, an obvious question would be to find out what this limit distribution is.

3 Proof of Theorem 1

For $x \in \mathbb{Z}_q$ and $\vec{i} = \{i_1, \dots, i_k\} \in \{0, \dots, L\}^k$ a vector of indices, let $A_{\vec{i}}^x$ be the event $i_1 g_1 + i_2 g_2 + \dots + i_k g_k = x \pmod{q}$. Let $A_L^x = \bigcup_{\vec{i} \in L^k} A_{\vec{i}}^x$ and let $A_L = \bigcap_{x \in \mathbb{Z}_q} A_L^x$. We abuse the notation and identify an event with its indicator function.

If A_L occurs then the diameter of the Cayley graph is at most kL , while if A_L doesn't occur then the diameter is at least L , which is the same order of magnitude, since k is fixed. Therefore, to prove both theorems it is enough to bound $\mathbb{P}(A_C \nmid \overline{q})$ from above and below.

Obviously, for any $\vec{i} \neq 0^k$ and any $x \in \mathbb{Z}_q$ we have $\mathbb{E}(A_{\vec{i}}^x) = 1/q$.

Next we want to calculate $\mathbb{E}(A_{\vec{i}}^x A_{\vec{j}}^x)$. This is the same as asking how many solutions, in $(\mathbb{Z}_q)^k$, are there for:

$$i_1 g_1 + i_2 g_2 + \dots + i_k g_k = x$$

$$j_1 g_1 + j_2 g_2 + \dots + j_k g_k = x$$

If \vec{i} and \vec{j} are linearly independent over \mathbb{Z}_q then the number of solutions is exactly q^{k-2} . In that case $\mathbb{E}(A_{\vec{i}}^x A_{\vec{j}}^x) = 1/q^2$ and therefore the events are independent. If \vec{i} and \vec{j} are linearly dependent over \mathbb{Z}_q then $\vec{i} = \lambda \vec{j}$ for some $\lambda \neq 1$. In that case there are no solutions since $x \neq \lambda x$ (except for $x = 0$ which we can ignore). Therefore, in that case

$$\text{Cov}(A_{\vec{i}}^x, A_{\vec{j}}^x) = \mathbb{E}(A_{\vec{i}}^x A_{\vec{j}}^x) - \mathbb{E}(A_{\vec{i}}^x) \mathbb{E}(A_{\vec{j}}^x) = 0 - 1/q^2 < 0.$$

Let $B_L^x = \sum_{\vec{i} \in L^k} A_{\vec{i}}^x$. Notice that $A_L^x = 0$ if and only if $B_L^x = 0$. By linearity of expectation,

$$\mathbb{E}(B_L^x) = \sum_{\vec{i} \in L^k} \mathbb{E}(A_{\vec{i}}^x) = \frac{L^k}{q}.$$

$\text{Var}(A_i^x) = \frac{1}{q}(1 - \frac{1}{q}) < \frac{1}{q}$ and $\text{Cov}(A_i^x, A_j^x) \leq 0$, giving

$$\text{Var}(B^x) = \sum_{\bar{i} \in L^k} \text{Var}(A_{\bar{i}}^x) + \sum_{\bar{i} \in L^k} \sum_{\bar{i} \neq \bar{j} \in L^k} \text{Cov}(A_{\bar{i}}^x, A_{\bar{j}}^x) < \frac{L^k}{q}.$$

Chebyshev's inequality now yields

$$\mathbb{P}(B_L^x = 0) \leq \mathbb{P}(|B_L^x - \mathbb{E}(B_L^x)| \geq \mathbb{E}(B_L^x)) \leq \frac{\text{Var}(B_L^x)}{\mathbb{E}(B_L^x)^2} < \frac{L^k/q}{(L^k/q)^2} = \frac{q}{L^k}$$

and therefore

$$\mathbb{P}(A_L^x) = 1 - \mathbb{P}(B_L^x = 0) \geq 1 - \frac{q}{L^k}$$

Let $T_L = \{x|A_L^x\}$ be the set of all points in \mathbb{Z}_q that can be reached by using each generator at most L times, and let $B_L = |T_L| = \sum_{x \in \mathbb{Z}_q} A_L^x$. Fix $C > 0$ and let $L = C \sqrt[k]{q}$. We now have $\mathbb{P}(A_L^x) \geq 1 - \frac{q}{L^k} = 1 - \frac{1}{C^k}$. Therefore $\mathbb{E}(B_L) \geq q(1 - \frac{1}{C^k})$. Since $B \leq q$, we can use Markov's inequality on $q - B_L$ to get

$$\mathbb{P}(B_L > \frac{q}{2}) = 1 - \mathbb{P}(q - B_L > \frac{q}{2}) \geq 1 - \frac{\frac{q}{2}}{\frac{q}{2}} = 1 - \frac{2}{C^k}.$$

Now if $B_L > \frac{q}{2}$ then for every $x \in \mathbb{Z}_q$ we have $T \cap (x - T) \neq \emptyset$. This means that A_{2L} occurs and therefore the diameter is at most $2kL$.

Therefore,

$$\mathbb{P}(\text{Diam}(q, k) > C \sqrt[k]{q}) \leq \mathbb{P}(B_{(C/2k) \sqrt[k]{q}} > \frac{q}{2}) \leq \frac{2}{(C/2k)^k} \xrightarrow{C \rightarrow \infty} 0$$

as required. ■

4 Proof of Theorem 2

Fix some $D < 1$ and let $L = D \sqrt[k]{q}$. Consider the events A_i^0 and A_L^0 as previously defined. As before, if \bar{i} and \bar{j} are linearly independent over \mathbb{Z}_q then $A_{\bar{i}}^0$ and $A_{\bar{j}}^0$ are independent events. If \bar{i} and \bar{j} are linearly dependent then $A_{\bar{i}}^0$ and $A_{\bar{j}}^0$ are in fact the same event. How many distinct events do we have among $\{A_{\bar{i}}^0\}_{i \in L^k}$?

Lemma 4 *There are at least $L^k/2 = D^k q/2$ such distinct events.*

Proof. Let \bar{i} and \bar{j} be linearly dependent, i.e. there exist $c \in \mathbb{Z}_q$ such that $\bar{i} = c\bar{j}$. In particular $i_0 = cj_0 \pmod{q}$ and $i_1 = cj_1 \pmod{q}$. eliminating c , we get $i_0j_1 = i_1j_0 \pmod{q}$. Since i_0, i_1, j_0 and j_1 are all less than \sqrt{q} (since $k \geq 2$) we get $i_0j_1 = i_1j_0$.

Take all $\bar{i} \in L^k$ for which i_0 and i_1 are coprime in \mathbb{Z} . If i_0 and i_1 are coprime and j_0 and j_1 are coprime and $i_0j_1 = j_0i_1$ then $i_0 = j_0$ and $i_1 = j_1$. Therefore, among the vectors considered above every two are linearly independent, so the corresponding events are distinct.

Given L how many pairs $i_0, i_1 < L$ are coprime? It is a well known fact (see [4]) that the fraction of coprime pairs tends to, and is always greater than, $6/\pi^2 > 1/2$. ■

Let $I \subset L^k$ be a set of index vectors such that every two are linearly independent and $|I| = \lceil D^k q/2 \rceil L$. Let $X = \sum_{\bar{i} \in I} A_{\bar{i}}^0$ and notice that $\mathbb{P}(A_L^0 \geq \mathbb{P}(X > 0))$.

Lemma 5 $\mathbb{P}(X > 0) > D^k/3$

Proof. For all $\bar{i} \in I$ we have $\mathbb{E}(A_{\bar{i}}^0) = \frac{1}{q}$ so

$$\mathbb{E}(X) = \frac{D^k q}{2} \frac{1}{q} = \frac{D^k}{2}$$

and these events are pairwise independent, so

$$\mathbb{E}(X^2) = \frac{D^k q}{2} \frac{1}{q} + \frac{D^k q}{2} \left(\frac{D^k q}{2} - 1 \right) \frac{1}{q^2} = \frac{D^k}{2} \left(1 - \frac{1}{q} + \frac{D^k}{2} \right)$$

Since X is nonnegative, from Cauchy-Schwartz inequality we get

$$\mathbb{E}(X)^2 = \mathbb{E}(X 1_{X>0})^2 \leq \mathbb{E}(X^2) \mathbb{E}((1_{X>0})^2) = \mathbb{E}(X^2) \mathbb{P}(X > 0)$$

and therefore

$$\mathbb{P}(X > 0) \geq \frac{\mathbb{E}(X)^2}{\mathbb{E}(X^2)} = \frac{\frac{D^{2k}}{4}}{\frac{D^k}{2} \left(1 - \frac{1}{q} + \frac{D^k}{2} \right)} \geq \frac{D^k}{3}$$

as required. ■

From lemma 5 we get that the probability of A_L^0 is bounded away from 0 regardless of q . Next we shall show that if A_L^0 occurs then many different \bar{i} yield the same member of Z_q , in which case the diameter cannot be too small.

Lemma 6 *Let C be such that $kDC^{k-1} < 1$. If $A_D^0 \sqrt[k]{q}$ occurs then*

$$\text{Diam}(q, k) > C \sqrt[k]{q} .$$

Proof. Let $L = D \sqrt[k]{q}$ and let $\bar{i} \in \{0, \dots, L\}^k$ be such that A_i^0 occurs. If \bar{j} and \bar{j}' differ by a multiple of \bar{i} then

$$j_1 g_1 + j_2 g_2 + \dots + j_k g_k = j'_1 g_1 + j'_2 g_2 + \dots + j'_k g_k \pmod{q} .$$

Therefore for every $\bar{j} \in \{0, \dots, L\}^k$ there exists \bar{j}' such that

$$j_1 g_1 + j_2 g_2 + \dots + j_k g_k = j'_1 g_1 + j'_2 g_2 + \dots + j'_k g_k \pmod{q}$$

and $j'_n \leq D \sqrt[k]{q}$ for some $1 \leq n \leq k$. The number of such \bar{j}' is bounded by $kD \sqrt[k]{q} (C \sqrt[k]{q})^{k-1} = kDC^{k-1}q < q$. Therefore, if $A_D^0 \sqrt[k]{q}$ occurs not all vertices are covered by combinations in $\{0, \dots, C \sqrt[k]{q}\}^k$ and hence the diameter is at least $C \sqrt[k]{q}$. ■

To wrap up the proof, given C , let $D = 1/(2kC^{k-1})$. From lemma 5 we conclude that $A_D^0 \sqrt[k]{q}$ occurs with probability at least $D/3$, in which case, by lemma 6 we get $\text{Diam}(q, k) > \sqrt[k]{Cq}$. ■

Acknowledgements

The authors thank Itai Benjamini, for suggesting this problem and for useful discussions.

References

- [1] N. Alon, Y. Roichman (1994) Random Cayley graphs and expanders. *Random Structures and Algorithms*, **5**(2), 271-284

- [2] M. V. Hildebrand (2005) A survey of random random walks on finite groups. *Probability Surveys* 2, 33-63
- [3] M. V. Hildebrand (1994) Random walks supported on random points of $\mathbb{Z}/n\mathbb{Z}$. *Probability Theory and Related Fields* 100, 191-203
- [4] D. Wells (1986) The Penguin Dictionary of Curious and Interesting Numbers. Middlesex, England: Penguin Books, 28-29
- [5] D.B. Wilson, Random random walks on \mathbb{Z}_2^d . *Probability Theory and Related Fields* 108 (1997), no. 4
- [6] Y. Roichman, On random random walks. *Ann. Probab.* 24 (1996), no. 2, 1001–1011.